*FSH SUPPLEMENT 1 TO AR 380-5

DEPARTMENT OF THE ARMY
HEADQUARTERS, FIFTH U. S. ARMY
AND FORT SAM HOUSTON
Fort Sam Houston, Texas 78234-5000
24 July 1989

Security
DEPARTMENT OF THE ARMY INFORMATION SECURITY PROGRAM

SUPPLEMENTATION. Further supplementation of this regulation is prohibited without prior approval of Commander, USAG, FSH.

SUGGESTED IMPROVEMENTS. The proponent for this supplement is the Directorate of Plans, Training, Mobilization and Security. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Cdr, Fifth U. S. Army and Fort Sam Houston, ATTN: AFZG-PTM-S, Fort Sam Houston, Texas 78234-5000

AR 380-5, Department of the Army Information Security Program Regulation, 25 February 1988, as supplemented by FORSCOM Supplement 1, 15 December 1988, is further supplemented as follows:

Page 4, Appendices. Add the following:

Appendix BB (Sample Emergency Evacuation/Destruction Plan)

Appendix CC (SAEDA Briefing).

Appendix DD (Entry/Exit Inspection Sign).

Appendix EE (Sample Record of Issue of DD Form 2501)

Paragraph 1-201, Applicability. Add subparagraph e:

e. This supplement, along with AR 380-5 and FORSCOM Supplement 1 to AR 380-5, applies to all military and civilian personnel under the jurisdiction of the Commander, USAG, Fort Sam Houston (HQ, USAG, FSH).

Paragraph 1-600b, Delegation of Classification Authority. Add subparagraph 5.

5. No office or individual has been delegated original classification authority for any level of classified information at HQ, USAG, FSH. All classified documents originated within HQ, USAG, FSH will either be derivatively classified or classified IAW classification guides and/or regulations. If a person not authorized to classify originates or develops information he or she believes should be safeguarded, the guidance in paragraph 2-600, AR 380-5, will apply.

This supplement supersedes FSH Suppl 1 to AR 380-5, 31 March 1986

Paragraph 2-103, Challenges to Classification. Add subparagraph g:

g. Individuals authorized access to classified information will be cognizant of the procedures for challenging classifications. DA Form 1575 (Request for/or Notification of Regrading Action) will be forwarded thru HQ, USAG, FSH, ATTN: AFZG-PTM-S when a challenge is desired.

Paragraph 2-212, Extracts of Information. Add subparagraph d:

d. When guidance is obtained from the classifier of source material, such documentation will be maintained with the file or record copy of the extracted information.

Paragraph 2-600, Procedures. Add subparagraph f:

f. Request for classification evaluation will be forwarded thru HQ, USAG, FSH, ATTN: AFZG-PTM-S, to the appropriate classification authority.

Paragraph 5-101, Standards for Storage Equipment. Add the following:

On Fort Sam Houston, the S&G Model 8077A Combination Padlock will not be used in any way to secure classified material.

Paragraph 5-102, Storage of Classified Information. Add subparagraph f:

f. Storage Authority:

(1) Activities storing classified material must have written authorization from HQ, USAG, FSH, ATTN: AFZG-PTM-S, to store such material. Requests for such authority will be submitted to the above office and will contain the following information:

Classification level of holdings to be maintained.

Type material to be maintained.

(c) Type security container to be used for storage, to include FSN/NSN.

Location of container (room and building number).

(2) Upon receipt of such requests, representative(s) of the Security Division, DPTMSEC will conduct a physical check of the desired classified holding area(s) to ensure compliance with applicable guidelines/regulations. Upon conclusion, a determination will be made, and if area meets minimum standards, written authorization will be furnished to store the classified holdings.

Paragraph 5-104b1, Changing. Add subparagraph h:

h. The Security Division, DPTMSEC, will provide assistance in changing combinations, if required. The same office will be notified if there is a safe lockout, malfunction, or indication of possible malfunction. (See app I, AR 380-5, for malfunction indicators).

Paragraph 5-104b3(d), Recording Storage Facility Data. Add the following to the information added by FORSCOM Supplement 1:

Combinations to all master/control containers will be stored with the Command Document Custodian, Directorate of Information Management (DOIM), or with a higher headquarters when approved by the Security Division, DPTMSEC.

Paragraph 5-105, Repair of Damaged Security Containers. Add subparagraph e:

e. All repairs to damaged security containers will be checked by the Security Division, DPTMSEC, prior to the container being placed back into service.

Paragraph 5-106, Turn In or Transfer of Security Equipment. Add the following to the information added by FORSCOM Supplement 1:

Security Division, DPTMSEC, will be notified in writing of all transfers or turn in of security equipment.

Paragraph 5-200, Custodial Precautions. Add subparagraphs h, i and j:

h. Command Classified Document Custodian. DOIM will appoint, in writing, a custodian of classified material for HQ, USAG, FSH. The Command Security Manager will establish requirements and other procedures to be used by the Command Custodian in locating and protecting classified material.

i. Unit/Activity Classified Document Custodians. Unit/activity classified document custodians will be appointed in writing for all units/activities which store or otherwise maintain classified materials. Custodians will be selected on the basis of experience and reliability and will maintain a security clearance at least equal to the highest classification of material for which the unit/activity is approved to store or maintain. Based on the volume of classified holdings, the document custodian may also be designated as the unit/activity security manager. A copy of the orders appointing custodian(s) will be forwarded to the HQ, USAG, FSH, ATTN: AFZG-PTM-S.

j. Activities which maintain small amounts of classified holdings should coordinate with the Command Document Custodian for storage of documents at the DOIM. Requests for such storage will be forwarded through HQ, USAG, FSH, ATTN: AFZG-PTM-S, to the Director, DOIM, ATTN: Security Manager/Command Document Custodian. Written approval will be granted by the DOIM Security Manager and the Installation Security Manager at which time the activity requesting storage will designate the Command Document Custodian as the activity document custodian by written appointment. Additional guidance for storage will be included in the written approval. This does not negate the activity or unit's responsibility for review of these documents at least annually.

Paragraph 5-203a, Emergency Planning. Add the following to the information added by FORSCOM Supplement:

Appendix BB contains a sample emergency evacuation/destruction plan. Each activity should use this plan or develop another plan to meet specific situational requirements. Each activity which modifies or develops additional plans will provide one copy to HQ, USAG, FSH, ATTN: AFZG-PTM-S.

Paragraph 5-203d, Emergency Planning. Add subparagraph 8.

8. Each activity which stores classified holdings will maintain emergency evacuation containers. Single drawer, easily transportable safes should be employed when available. When the volume of classified holdings is small, large opaque envelopes may be used, otherwise collapsible corrugated shipping boxes should be procured. When boxes or envelopes are identified as evacuation containers, they will be maintained at or near the permanent security container and designated for emergency use by affixing a 3x5 card which reads, "Emergency Evacuation Container for Classified Documents", accompanied by organization/activity identification. Packing tape or twine will also be maintained to seal containers.

Paragraph 5-205d2m, Security of Meetings and Conferences. Add subparagraphs n, o & p:

n. As HQ, USAG, FSH does not maintain an approved secure briefing area, requests for the use of uncleared facilities for classified meetings will be forwarded to the Security Division, DPTMSEC, not later than ten working days prior to the scheduled meeting. Requests to conduct regularly scheduled or recurring classified meetings will be submitted annually to HQ, USAG, FSH, ATTN: AFZG-PTM-S. As a minimum, requests will contain the following information:

Date, time, place and duration of meeting.

Activity point-of-contact sponsoring the meeting

(3) Highest level of classified information to be discussed.

(4) Security measures coordinated for the meeting.

o. The sponsoring activity will provide guards at all entrance/egress locations to/from the briefing area to control access at all meetings where classified information will be discussed. When available, appropriately cleared Military Police personnel should be utilized as coordinated between the sponsoring activity and PMO. When PMO personnel are not available, properly cleared personnel other than Military Police may be employed. Control personnel will ensure that no unauthorized personnel loiter in the immediate area.

p. Access to classified meetings and conferences must be strictly controlled. Roster of Personnel Authorized Access to Classified Information, validated by the Chief, Security Division, DPTMSEC, is the only access roster authorized for use within HQ, USAG, FSH. Proper identification will be compared against access roster prior to granting individual access to the classified briefing area. Access will be denied to any individual not listed on this form until verification is received from the Security Division, DPTMSEC, by the most expeditious means.

Paragraph 5-300g1(i), Activity Entry and Exit Inspection Program. Add the following paragraphs:

(1) As a minimum, entry/exit inspections will be conducted at the following activities:

ACTIVITY	LOCATION	DIRECTORATE
Security Division	Bldg 258	DPTMSEC
Photo Branch, TSC	Bldg 2001	DPTMSEC
P&O Division	Bldg 155	DPTMSEC
Mob Division	Bldg 300	DPTMSEC
P&O Division	Bldg 2250	DOL
Maint Division	Bldg 371	DOL
Sup & Svcs Division	Bldg 4015	DOL
Ops Section	Bldg 3520	507th MD Co
S2/3	Bldg 2265	41st CSH
Message Center	Bldg 366	DOIM
Communications Center	Bldg 16	DOIM
Computer Center	Bldg 4190	DOIM
HF Radio Station	Bldg 1980	DOIM
546th EOD	Bldg 2061	
137th EOD	Bldg 612A	

(2) The following criteria will be used in determining the minimum number of hours entry/exit inspections will be conducted during each quarter:

(a) Facilities which store, process or handle less than one linear foot of material classified SECRET or CONFIDENTIAL will be subject to a maximum of one hour of entry/exit inspections each quarter.

(b) Facilities which store, process or handle more than one linear foot of material classified SECRET or CONFIDENTIAL will be subject to a maximum of six hours of entry/exit inspections each quarter.

(c) Facilities which store, process or handle any amount of TOP SECRET or special access material will be subject to a maximum of eight (8) hours of entry/exit inspections each quarter.

(d) During EOC activations, a minimum of one hour of entry/exit inspection will be conducted for each 24 hour period of EOC activation.

(3) All entry/exit inspections will be scheduled and conducted by Security Division personnel. These inspections will be unannounced.

(4) Signs will be posted in the immediate vicinity of the entry/exit inspection point during the inspection. These signs will be similar to the sign at appendix DD.

(5) The Security Division, DPTMSEC is designated as the Control Office for all inspections of this type. Personnel discovered with classified material and no Courier Authorization Card (DD Form 2501) will be referred to the Control Office for further disposition. Inspectors who made the discovery will obtain the individual's name, grade, SSN and office of assignment as well as identifying data of the document(s) in the individuals possession (subject, office symbol, date and classification). This information will be relayed to the Control Office as quickly as possible and will be noted in the report of the entry/exit inspection.

Paragraph 5-302b2, Inspection Procedures and Identification. Add subparagraphs (i), (j) and (k) after subparagraph (h) added by FORSCOM supplement 1:

(i) DD Forms 2501 (Courier Authorization Cards) for HQ, USAG, FSH will be issued for the "Greater San Antonio, Texas area", which includes Camp Bullis, Camp Stanley, Kelly, Randolph, Lackland and Brooks Air Force Bases. These cards are not valid outside this area.

(j) The Installation Security Manager, DPTMSEC, will issue DD Forms 2501, by serial number, to all subordinate security managers of HQ, USAG, FSH activities. Security managers will control issue of these forms to individuals having a need for a Courier Authorization Card. A record of each card issued will be maintained. Appendix EE contains a sample record of issue format.

(k) Individuals from Defense Mapping Agency and Special Security Office activities at Fort Sam Houston, who are carrying SCI material may request exemption from inspection to preclude "inadvertent disclosure" or compromise of this material. Courier Authorization Cards for these individuals will be overstamped with a notification exempting the bearer from inspection and must be used in conjunction with SCI Courier Orders issued by the local Special Security Officer. Personnel from the 902d MI, who are carrying SAP material will also be issued overstamped DD Forms 2501, and may request exemption from entry/exit inspections when required. These overprinted courier cards will be controlled and issued by the Installation Security Manager.

Paragraph 6-105, Responsibility of Authority Ordering Investigation. Add subparagraph g:

g. Within HQ, USAG, FSH, informal inquiry UP AR 15-6 and any other investigations will be ordered by the Garrison Commander or Deputy Garrison Commander only.

Paragraph 7-300f, Transfer of Accountability. Add subparagraph 4:

4. As a minimum, three copies of the joint inventory will be completed. One copy will be retained by the departing TSCO one copy will be maintained on file in the activity, and one copy will be forwarded to the Security Division, DPTMSEC.

Paragraph 7-301, Secret Information. Add subparagraphs e and f after subparagraph d added by FORSCOM Supplement 1.

e. Although administrative accountability records keeping has been relaxed, the requirements for protection of classified information from unauthorized disclosure remain in effect. Enforcement of official need-to-know controls and physical safeguards remain. Controls on hand carrying, transmission, identity and authorized access of recipients, removal of documents from government facilities, and reproduction controls also remain in effect. A listing of secret documents will be used to facilitate filing and retrieval.

f. When a classified document is received from another headquarters and not routed thru the DOIM and an acknowledgment of receipt is requested or required, the receiving unit/activity

will hand carry the material and the receipt to the DOIM for processing.

Paragraph 7-305, Restraint or Reproduction. Add the following:

Classified material will only be reproduced on equipment under the control of DOIM. Requests for exception to this policy will be forwarded to Security Division, DPTMSEC, with full justification and classified reproduction capability explanation.

Paragraph 7-305b. Add the following:

The Installation Security Manager, Security Division, DPTMSEC, is appointed as the official authorized to approve reproduction of SECRET information. Units/activities requiring copies of such material will hand carry the material to the Security Division, DPTMSEC, accompanied by DD Form 844 (Requisition for Local Duplicating Service), signed by the director, staff section chief, or unit/activity security manager. Once approved, the material will be taken to the DOIM for reproduction. Requests for exceptions to this policy will be forwarded to the Security Division, DPTMSEC. Unit/activities (who have reproduction authority, see 7-305 above) security managers are authorized to approve reproduction of confidential material.

Paragraph 8-102, Secret Information. Add subparagraph i:

i. All secret material mailed from this headquarters will be coordinated with the Command Document Custodian. Unit/activity security managers will ensure compliance with paragraphs 8-200 and 8-202, AR 380-5, regarding mailing of classified material.

Paragraph 8-303a1. Add the following:

Written requests will be forwarded to the Security Division, DPTMSEC, and will include the information in figure 8-2, FORSCOM Supplement 1, this regulation. Once approved, the request will be coordinated with the authorized travel order approving official and a copy provided as an enclosure/amendment to the travel order.

Paragraph 9-101, Method of Destruction. Add the following:

Classified material will be destroyed in the post disintegrator building 4224, or by other approved means defined in appendix I, AR 380-5. The unit/activity security manager, classified custodian, or other properly cleared individual will hand carry material to the destruction facility and will remain with the material until destruction is confirmed. If continuous strip shredders are used to destroy classified material, the 'Secure

Volume' concept will be strictly enforced. (See para K-2a, appendix K, AR 380-5). No new continuous strip shredders will be obtained. The post disintegrator is approved for destruction of all levels of classified material and is available for use of all Fort Sam Houston activities and tenants. Use of this activity will be coordinated thru the Security Division, DPTMSEC.

Paragraph 9-104, Classified Waste. Add the following:

Within HQ, USAG, FSH, classified waste will not be retained longer than 30 days. Such waste will be stored in an approved security/storage container until destruction is effected.

Paragraph 10-101, Scope and Principles Add subparagraph n:

n. Within this headquarters, all personnel authorized access or expected to be authorized access to classified information will receive a security briefing from the unit/activity security manager within 30 days of arrival in the unit/activity and/or prior to actual access to classified information. Refresher briefings, IAW paragraph 10-102, will be conducted at least annually thereafter. In addition to the briefing requirements of paragraph 10-101, specific security responsibilities and unique unit/activity procedures will be defined.

Paragraph 10-104a, Foreign Travel Briefing. Add subparagraph 4 after subparagraph 3 added by FORSCOM Supplement 1.

4. The Security Division, DPTMSEC, will conduct foreign travel briefings for all personnel of this headquarters as required or requested. Unit/activity security managers will coordinate with the Security Division, DPTMSEC for scheduling of these briefings.

Paragraph 10-105, Termination Briefings. Add subparagraph g and h:

g. The Security Division, DPTMSEC, will conduct termination briefing of all personnel whose clearance has been revoked.

h. Preparation, completion, and filing of DA Form 2962 personnel terminating employment will be accomplished by the activity Security Manager.

Paragraph 13-304c, Field Program Management. Add the following:

The Chief, Security Division, DPTMSEC, will be appointed as the Security Manager for Headquarters, USAG, Fort Sam Houston. Each unit, directorate, and separate agency or activity of HQ, USAG, FSH, will appoint a security manager to administer the Information Security Program (ISP) with that organization. Commanders, directors, and chiefs of activities may appoint additional security managers in subordinate elements to assist

in administering the ISP if warranted by the location, size, or function of the subordinate element. A copy of all security managers' appointment orders will be forwarded to the HQ, USAG, FSH, ATTN: AFZG-PTM-S.

Paragraph 13-304c1(h), Field Program Management. Add the following to subparagraph (1) added by FORSCOM Supplement 1:

The Security Division, DPTMSEC, will conduct annual security inspections of all units, directorates, and activities within HQ, USAG, FSH. A copy of the inspection report will be forwarded to the inspected activity where it will be maintained until receipt of the next equivalent inspection report.

Paragraph 14-104a, Reporting Violations. Add the following:

Reports of violations, as described in paragraph 14-101 above, will be forwarded thru the Security Division, DPTMSEC.

FOR THE COMMANDER:

OFFICIAL:

GEORGE A. FINLEY
Director of Information Management

GEORGE A. FINLEY
Director of Information Management

DISTRIBUTION:
A
B
25 - AFZG-PTM-S
25 - AFZG-IM-LSBP

APPENDIX BB

SAFE REMOVAL & DESTRUCTION OF CLASSIFIED MATERIAL

1. IN CASE OF FIRE OR NATURAL DISASTER REQUIRING IMMEDIATE EVACUATION OF THE BUILDING:

If possible, all classified material will be returned to the security container, and the container locked prior to evacuation. Where the danger is so imminent that a delay will threaten the safety of personnel, the security containers will be locked and personnel will carry any classified material in their possession out with them as they evacuate.

2. IN CASE OF CIVIL DISTURBANCE, TERRORIST ACTIVITIES, ENEMY ACTION, OR OTHER EMERGENCY CONDITIONS REQUIRING RELOCATION OF CLASSIFIED MATERIAL:

a. Safe removal of classified material will be accomplished only upon the order of the Commander, USAG, Fort Sam Houston or the following designated representatives:

Deputy Garrison Commander

USAG Staff Duty Officer

(3) Director of Plans, Training, Mobilization and Security.

Staff Directors.

Chief, Security Division, DPTMSEC.

b. Once ordered, the following personnel are responsible for accomplishing the safe removal of classified material (See attached list):

Activity Security Manager.

Custodian of Classified Documents.

Senior properly cleared person present.

Alternate responsible personnel, properly cleared.

c. If the order to implement the safe removal plan is received telephonically, the responsible individual (paragraph b, above) should verify the order by return call if there is any doubt concerning the authenticity of the order.

d. To effect safe removal, all classified material will be placed in emergency evacuation containers. Classified material will be removed from the security containers in accordance with the priority assigned to each drawer or container. The emergency evacuation containers will be moved in accordance with instructions provided by the official directing the action. (NOTE: Each activity will establish a primary and alternate evacuation site and will document at least one practice evacuation annually). Upon evacuation, the emergency evacuation containers will be accompanied by one of the individuals listed in paragraph 2b, above. Further instructions will be furnished at the evacuation site.

3. IN CASE OF EMERGENCY DESTRUCTION:

When emergency destruction is ordered, the post disintegrator, bldg 4224, will be used, time permitting. The post incinerator will be used in an emergency situation to assist in the rapid destruction of classified material. Local destruction by alternate methods will be authorized only by those individuals listed in paragraph 2a, above. If local destruction is authorized, material will be destroyed in accordance with the priorities listed on the security container. Local destruction will be accomplished by personnel listed in paragraph 2b, above and without regard to pollution, preventive maintenance or other environmental constraints.

4. The Chief, Security Division, DPTMSEC, will be notified immediately upon completion of all directed emergency evacuation or destruction actions.

5. References:

a. Paragraph 5-2Ø3, AR 38Ø-5, Department of the Army Information Security Program.

b. FORSCOM Supplement 1 to AR 38Ø-5

c. FSH Supplement 1 to AR 38Ø-5

PERSONNEL RESPONSIBLE FOR REMOVAL/
DESTRUCTION OF CLASSIFIED MATERIAL

ACTIVITY _____

TITLE	NAME	DUTY POSITION
Security Manager		
Document Custodian		
Alternate		
Alternate		
Alternate		

Figure BB-1. Sample Format for Attachment to Safe Removal & Destruction of Classified Documents Plan

APPENDIX CC

SAEDA BRIEFING

Regardless of our duties, each of us possesses information of value to hostile intelligence. The purpose of this Subversion and Espionage Directed Against the U. S. Army (SAEDA) is to acquaint you with methods used by hostile intelligence services (HOIS) to obtain information and your responsibility to report any actual or suspected approach by a foreign agent. First, it is important to understand each of the elements we are discussing.

1. SUBVERSION: Is the attempt by an individual or group to undermine our faith and allegiance in our government, our nation or the American way of life.

2. ESPIONAGE: Is the practice of obtaining, transmitting, or receiving information concerning national defense or security with the intent of assisting a foreign power.

3. DIRECTED AGAINST THE U. S. ARMY: This not only includes those in uniform, but civilian employees and dependents of military and civilian employees.

4. DELIBERATE SECURITY VIOLATION: This is when an individual who has been placed in a position of trust and responsibility with the U. S. Government deliberately and willingly discloses classified defense information to a person or organization, which is not authorized access to such information. A deliberate security violation is punishable by a $1Ø,ØØØ.ØØ fine, 1Ø years in prison, or both. Other higher penalties can, and have been imposed.

History has demonstrated that this country's Armed Forces members, civilian employees, and their dependents are prime targets of hostile intelligence services. For that reason, it is important to remember that we are all potentially subject to approach regardless of our location. Human intelligence agents are active against the U. S. Military overseas and in the Continental United States.

The FBI Special Agent had been trailing the blue and silver Astrovan for over an hour when it came to a fork in the road. The left fork branched off into the mountains of western Virginia, the right continued on to Washington, D. C. The van took the right fork, and the Special Agent lit up a cigar in satisfaction, his first cigar in several months.

Why the satisfaction? The driver of the van was John A. Walker, who was suspected of spying for the Soviets. The FBI

had received a tip from Walker's ex-wife, and had him under surveillance for months. On this May afternoon in 1985, when John Walker left his home in Norfolk, Virginia, the FBI suspected that he might be heading for Washington, D. C., to meet with a KGB officer assigned to the Soviet Embassy. The FBI was right, the chase was on.

A team of FBI Special Agents and investigative support personnel tracked Walker to a remote location in the Maryland suburbs of Washington where he stopped his van near a road sign, got out, and stashed a paper shopping bag in the woods. When the bag was retrieved by FBI personnel they were startled by its contents. Inside were dozens of classified U. S. Government documents. The FBI followed Walker to a motel where he was arrested for espionage.

That afternoon a Soviet Embassy official had been seen in the area where Walker had left the shopping bag. He was Aleksey G. Tkachenko, a known KGB officer. Tkachenko apparently sensed that something was wrong and had returned to Washington without attempting to pick up Walker's package. A few days later, his tour of duty was terminated prematurely and he returned to the USSR.

The Walker case is just one of the many espionage operations that have been uncovered and neutralized in recent years.

Who are these spies standing trial for espionage? By far and away they're Americans--not foreigners. Eighteen of the 25 persons arrested in 1984 and 1985 were born in the United States. These figures are somewhat misleading, for during the same two-year period a number of Soviet officials were also observed in the act of committing espionage, but because they had diplomatic immunity were not arrested. Instead, they were sent home, never to return to continue their trade.

While it is true that many of the espionage trials received front-page coverage, the struggle between American counterintelligence forces and hostile foreign intelligence services remains, for the most part, unseen, shrouded in secrecy. The following information should shed some light on the targets and strategies of these foreign intelligence services and attempt to enlist informed citizens, particularly those of you having access to classified information, into this struggle.

THE THREAT:

The world of espionage and counterespionage is a popular subject of fiction. It has been the topic of innumerable books, short stories, television series, and movies. The role of the spy and "Secret Agent" has become so sensationalized and exaggerated that it is easy to think that spying belongs in the

same category as science fiction and adventure novels. Many Americans believe this simply because they don't know who the spies are or how they operate.

Who are these intelligence officers, and what are they after? The bulk of them are from the Soviet Union, but the USSR's allies in Eastern Europe, as well as Cuba, the People's Republic of China, and other nations also assign intelligence officers to the United States.

The foreign intelligence services assign intelligence officers to work in the United States, generally under the cover of an official or a visitor. These intelligence officers in turn operate "agents," most of them Americans, who collect information.

The main objective of these intelligence services is the wholesale collection of information. The most prized item, of course, is classified U. S. Government material. However, unclassified material can also be of inestimable value. Advanced U. S. technology, especially that which is barred for export to these countries, is a major intelligence target.

Since 1975, the number of communist country officials assigned to the United States has increased at a steady rate. It has been the experience of the FBI, confirmed by the counterintelligence services of our allies, that roughly one out of three communist country officials is an intelligence officer.

Furthermore, the number of business representatives, scholars, and the like from these countries has more than doubled since 1975. Many of these individuals work for or on behalf of their respective intelligence services, greatly increasing the potential for espionage operations.

From 1975 to 198Ø, there were 13 espionage arrests. From 1981 to 1985 there were 33 such arrests. This is a cause for alarm. It shows the capability of the Soviet KGB and other intelligence services to commit espionage in the United States.

Here are vignettes of some of the cases:

In late 1981, an American citizen, William Holden Bell, and a Polish intelligence officer were arrested and convicted of espionage after a large amount and variety of military technology was passed to Warsaw and, presumably, to Moscow.

In May 1984, James Durward Harper, an American businessman, was found guilty of espionage and sentenced to life imprisonment. Harper passed numerous classified documents concerning U. S. missile and other defense technology to Polish intelligence officers which, as in the Bell case, ended in the hands of the Soviets.

In the spring of 1985, Thomas Patrick Cavanagh, an engineering specialist at Northrop Corporation, was sentenced to life imprisonment after he attempted to sell classified documents from the "Stealth Bomber" project.

In 1985, John Anthony Walker, Jr., Michael Lance Walker, Arthur James Walker, and Jerry Alfred Whitworth were arrested on espionage charges for their roles in passing classified information to the Soviet Union. All were convicted of those charges.

Also in 1985, retired Central Intelligence Agency (CIA) analyst Larry Wu-Tai Chin was arrested for supplying classified information to the People's Republic of China throughout most of his 33-year career. On February 1986, distraught over his conviction for espionage, Chin committed suicide in his jail cell.

In November 1985, Jonathan Jay Pollard, an intelligence analyst at the Naval Investigative Service (NIS), and his wife were arrested for espionage. Pollard provided classified information to the Israeli intelligence services. Both pled guilty to espionage charges in 1986.

In June 1986, Ronald William Pelton, a former National Security Agency employee, was found guilty of espionage. Pelton supplied the Soviets with extremely sensitive classified information for three years. Evidence leading to Pelton's arrest for espionage activity came from an unlikely source, a high-level officer who had defected to the United States.

Also in June of 1986, Richard W. Miller, a former Special Agent assigned to the FBI's Los Angeles Office, was found guilty of espionage. With the help of two Soviet emigres, who were also convicted of espionage, Miller passed classified information to the Soviet Union.

In most of these cases, considerable damage was done to the U. S. national security interests For instance, the CIA concluded that as a result of the Bell espionage case, the Polish and Soviet Governments would save "hundreds of millions" of dollars in research and development. The documents provided by Bell would enable them to implement proven designs developed by the United States and field operational counterpart systems in a much shorter period of time. Similarly, U. S. defense experts determined that the value of the information turned over to the Soviets and Poles by Harper was "beyond calculation." Fortunately, comparable damage was averted when the FBI arrested Thomas Patrick Cavanagh before he had the opportunity to pass any sensitive documents to a hostile intelligence service.

The need for similar damage assessments has been prevented more than once in recent years, thanks to concerned citizens like William H. Tanner, Jr.

In December 1981, Mr. Tanner agreed to assist the FBI and NIS in a joint investigation of the East German intelligence services (EGIS). Under the direction of the FBI and NIS, Mr. Tanner, posing as a disgruntled U. S. military officer, walked into the East German Embassy in Washington, D.C., and offered to sell classified U. S. documents.

The East Germans accepted his offer. Mr. Tanner met with the East Germans for several months, and in the summer of 1982, he was introduced to his "handler," Alfred Zehe, who is a physicist, a former exchange student in the United States, and an agent of the EGIS. For two years, Mr. Tanner worked as a double agent, meeting Zehe at different sites in Mexico City and Europe. At these meetings, Tanner turned over documents that had been authorized for release by the U. S. Government in exchange for $22,000 from the East Germans.

In November 1983, while attending a scientific conference in Boston, Massachusetts, Alfred Zehe was arrested for espionage by Special Agents of the FBI and subsequently convicted of espionage. In 1984, the East German Government released 23 individuals in exchange for Zehe and three other Soviet-Bloc spies.

With the assistance of Mr. Tanner, the FBI gained valuable counterintelligence information concerning EGIS techniques and operations. It was also firmly established that the EGIS utilize exchange students and professors in espionage activity.

During the course of the investigation, Mr. Tanner repeatedly exposed himself to personal danger, with no expectation of recognition or reward. In 1985, FBI Director William H. Webster presented Mr. Tanner with the Society of Former Special Agents annual award.

While newspapers feature stories of individuals who have literally sold out their country for personal financial gain, William H. Tanner, Jr., is an example of those patriotic Americans whose loyalty and honor cannot be purchased - a genuine "sentinel of freedom."

HOSTILE INTELLIGENCE SERVICES STRATEGY:

In their task of gathering information, the intelligence services have a large array of tools at their disposal. Satellites collect photographic and electronic data; aircraft and ships can also gather electronic intelligence; the human source fills the gaps. Some would argue that only the human source can discover intentions, but intentions must be communicated or they are nothing more than musings. Yet it often takes a human source to provide the key to unscrambling communications that are intercepted by sophisticated technology.

Probably the greatest achievement of an intelligence organization is the placement or recruitment of an agent in a sensitive position in a national defense or intelligence agency of another government. The penetration of private and commercial enterprises involved in sensitive defense research and development work can also be of great value. Americans who have been recruited by hostile intelligence services can also serve as middlemen to acquire technology that has been embargoed from export. Even if the American does not have access to classified material or embargoed technology, he can be used by hostile intelligence as a so-called "spotter," one who can supply personal data (perhaps unwittingly) about Americans who do have access to sensitive information.

The central mission of the hostile intelligence services in the United States is the assessment and recruitment of Americans as agents. To this end, intelligence officers and their agents are in frequent contact with Americans, evaluating them as potential recruitment targets. If he appears to have potential for development as an agent, several different techniques or approaches may be used to recruit him.

FINANCIAL CONSIDERATIONS/GREED:

The man appeared to be quite successful - he held a job as an engineer with a top U. S. defense firm and, on the surface, was a model citizen. This was not the case, however, for he was in deep financial trouble. But there was a way out of his difficulties. He had recently been befriended by an East European businessman who, upon hearing of the engineer's difficulties, offered monetary assistance. The price would be small - merely supply the businessman with unclassified technical data from the engineer's firm which he did.

The engineer later realized that even by supplying unclassified data he had compromised himself, and eventually his "friend" would request classified information. When this occurred, the engineer was able to rationalize his actions, and he continued to provide information for cash.

Needless to say, the East European "businessman" was no businessman, but a professional intelligence officer using his business association as a "cover" for clandestine intelligence collection. The engineer had become entangled in a full-fledged espionage operation. He was provided with concealment devices in which to hide stolen documents, he executed clandestine meetings overseas and before being arrested by the FBI, he had been paid in excess of $100,000 for his labors.

In another case, an American businessman hatched an idea that he believed would bring in some quick and easy profits. He would sell classified documents to a Soviet Bloc country.

The businessman had no access to classified material, but his girlfriend did. She worked at a firm involved in U. S. defense projects. Together they plotted and stole numerous Secret documents. The businessman then contacted agents of the Polish intelligence services.

Recognizing that the American was motivated largely by greed, the Polish intelligence officer preyed upon his weakness. The American was paid $15,000 for the initial documents and was promised much more if he continued to supply classified information. He did, and prior to his arrest by the FBI, he had been paid $250,000 by the Poles for sensitive documents. The material was so valuable that it was immediately turned over to the Soviets. The Polish intelligence officers who handled the American were promoted, and they received commendations from then - KGB chairman, Yuriy Andropov.

The American was convicted of espionage and is now serving a life sentence in a U. S. penitentiary.

Of the various tactics used by spies, those geared to exploit an American's material needs are perhaps the most common and effective. Many Soviet and other communist intelligence officers believe that Americans, as capitalists, are hopeless materialists who can be swayed by appeals to greed. In the early 1960s, a Western intelligence service obtained a copy of a KGB training manual used to train new officers prior to assignment in the United States. The following is a direct quote from the manual:

> "The successful use of financial motivation in recruitment requires above all an understanding of the psychological make-up of the average American. He seriously regards money as the only thing which can ensure his personal freedom and independence and make it possible for him to satisfy his material and spiritual needs. This typical American attitude toward money creates indifference to the means by which it is obtained, even though risk is sometimes involved."

BLACKMAIL/HOSTAGE SITUATION:

A U. S. Government employee, while traveling in the Soviet Union, was approached by an attractive woman. The exchange of conversation and the flow of vodka created an atmosphere which led the American to venture the proposition, "I suppose it's quite obvious that this representative of a decadent Western society would like to make love to you." The proposition was quickly, perhaps too quickly, accepted.

Little did the American realize that the woman was a KGB agent, and that the ensuing events of the evening were being filmed by the KGB. Little did he realize that hostile intelligence services use blackmail, and that he had become

involved in a classic, compromising situation. The situation left him vulnerable to a blackmail attempt by the KGB.

Luckily, the American blunted the threat of any KGB coercion by revealing the full details of his unfortunate encounter to Federal authorities upon his return to the United States.

Hostile intelligence services can play rough in their drive to compromise and recruit U. S. citizens visiting communist countries. Attempts to compromise Americans through sex and other ploys while they are touring the Soviet Union and other East European countries are not uncommon, particularly in the bars and cafes frequented by foreigners. On the other hand, such attempts within the United States are uncommon, although knowledge of any personal vulnerabilities of Americans is sought for exploitation abroad.

Another tactic employed by the hostile intelligence services is the exploitation of hostage situations. If a foreign intelligence service learns that a targeted individual has relatives overseas in their country of national origin, the individual is regarded as being in a potentially vulnerable hostage position. First will come gentle persuasion. An intelligence officer may produce a "letter" from relatives calling for the American to "cooperate." If that doesn't work, the intelligence officer may suggest that harsh measures could be applied to the relatives. An American who finds himself approached in this manner must make some difficult decisions, because the threat may be genuine. But if he yields to such a request or threat he runs the risk of becoming entangled in a very unpleasant experience.

APPEAL TO NATIONAL PRIDE:

An employee of a leading computer firm who was of East European descent was invited to tour his native country. Upon arriving in Eastern Europe, he was treated graciously by government officials and was provided with a personal "guide" to accompany him on the tour. The "guide" was in reality an operative of an East European intelligence service, whose assignment was to assess the visitor's potential for recruitment as an agent. A year after the computer specialist had returned to the United States, he was contacted by an official from his native country. The official arranged a luncheon date with the specialist. At lunch, he attempted to elicit information about computers by appealing to the specialist's pride in his native land.

The approach normally goes something like this:

"I know you're a good American, but I also know you love your homeland. You could really help your people

by sharing some of you expertise. Things are tough over there - you understand. We hope to rely on friends like you to help us move into the 2Øth Century."

This case has a positive outcome. Recognizing the irregularity of this contact, the computer specialist immediately contacted the FBI. This was fortuitous, for the official was, in actuality, an intelligence officer soliciting information normally restricted from him.

EXPLOITATION OF AN EMOTIONAL INVOLVEMENT:

A recent espionage case revolved around a U. S. Government employee who was recruited overseas and supplied classified documents and information to a foreign agent. What made this case unusual was the fact that the American received no monetary payment for her services. She engaged in espionage because she became romantically involved with an agent of a foreign intelligence service.

The young American was the product of a close-knit family and was reared in a small Virginia town. She had seldom traveled, and an assignment overseas was sure to produce culture shock.

Shortly after arriving at her new job, she met a native of that country, who was labeled by those who knew him as a "ladies man." A romance flowered between the two. The man nurtured the relationship for several months, and eventually determined that the woman had access to sensitive material. He began to exploit the relationship to obtain classified information and threatened to end their romance unless she cooperated. She did. The young woman provided information to the agent for over a year.

Upon returning to the United States, her activities were uncovered by U. S. Intelligence, and she was eventually convicted of espionage and sentenced to prison. The individual who recruited her was also arrested and convicted on espionage charges.

"FALSE FLAG" APPROACH:

In a false flag approach, a hostile intelligence officer may misrepresent himself as a citizen of a country friendly to the United States. Thus, a targeted American may be duped into handing over sensitive information by being led to believe that he is aiding an ally of the United States.

In a variation of this approach, an intelligence officer or agent poses as a representative of a noncommunist country or entity towards which an American is particularly sympathetic. This variation was used in a case involving an American of

Armenian extraction. He was approached by another Armenian who claimed to be a "distant relative." The relative said he was working for Armenia, with the assistance of the Soviet Union, in a drive to reclaim lost Armenian lands from Turkey. The distant relative was, in actuality, a KGB agent who eventually duped his target into giving him classified information.

APPROACHES BASED ON IDEOLOGY:

If a hostile intelligence service officer or agent believes that an individual has communist sympathies, he may make an appeal for information based on ideology. This type of approach is now less frequently observed than in the 1950s and 1960s. A "pitch" for information may also be geared to take advantage of an American's desire for international harmony and world peace. An intelligence officer can also exploit an American's concern for a single issue, such as nuclear disarmament, by claiming to have a similar concern, and thus ingratiate himself with the American.

An American scholar in Europe, sympathetic toward the Soviet Bloc, was approached by a hostile service. The scholar eventually agreed to cooperate with the service in working for "world peace and harmony." He became an agent of a communist country. When the scholar returned to the United States, at the direction of his handlers, he attempted to gain employment with the U. S. Government in a position that would give him access to highly sensitive data. Fortunately, his motives were uncovered.

EXPLOITATION OF AN AMERICAN'S NAIVETE:

This approach may be used against an impressionable individual. A common tactic for a hostile intelligence officer is to pose as a "student" or "researcher" and exploit traditional American beliefs, such as freedom of speech or the conviction that scientific advancements should be allowed to benefit all mankind in an attempt to elicit information. Their targets are usually American students, professors, or scientists. In some instances the Americans may not even have access to classified information. They are recruited by hostile intelligence services in the hope that they will eventually obtain jobs which afford them access to sensitive information. In many instances, the targeted American is not aware he is being recruited.

This type of recruitment approach is well exemplified by a recent case. In the spring of 1981, an American student was putting in a late evening, typing a paper in his dormitory room, when he heard a knock at his door. It was his next door neighbor, an exchange student from Bulgaria, complaining about the noise. The American apologized and later that week invited his disgruntled neighbor over for drinks. During the visit, the conversation turned to politics, with the American criticizing some of the policies of the current U.S. administration. At

that time, the American was not aware he was talking to an agent of the Bulgarian intelligence services.

One week later, the American was invited to the Bulgarian's room, where he was introduced to another guest, a Bulgarian trade official. In reality, this official was an intelligence officer who was responsible for monitoring Bulgarian student activities in the United States.

During the course of the evening, the Bulgarian official questioned the American extensively about his studies and finances. Before leaving, he asked the American to assist him in conducting research on some economic and technical subjects for a fee. The American, seeing no harm in this, agreed. He continued to conduct research for the Bulgarian official for almost a year without realizing that he had become a target for recruitment. As the American neared the end of his schooling, the Bulgarian official began to take an interest in his postgraduation plans.

Then something fortuitous occurred. The American watched a local television news program that dealt with KGB activities in the United States. As he watched it, he began to see many similarities between his developing relationship with the Bulgarian and the KGB recruitment techniques depicted in the program. This stark realization led him to contact the FBI.

With the American student's assistance, the FBI developed a counterintelligence operation that led to the arrest of the Bulgarian official for espionage.

REVENGE/DISAFFECTION:

An element which has been at the center of many espionage cases is revenge. Some disgruntled employees think that a quick way to wreak vengeance, and earn money as part of the bargain, is to sell valuable information to a hostile intelligence service.

The best example of the revenge motive in action occurred in the William Kampiles case. While still employed by the CIA, Kampiles had been told by his superiors that his chances for advancement were minimal due to his poor work performance. He then resigned in a huff from the CIA, stealing a highly sensitive and valuable classified document, which he sold to the Soviets. Certainly Kampiles gained some measure of revenge against the CIA, but in the process did grave harm to his country. As a result of his impulsive gesture, he was sentenced to 4Ø years in a Federal penitentiary.

COUNTERING THE THREAT:

There is a common notion that the KGB and other services are staffed with crude individuals, who have bushy eyebrows,

wear baggy suits, and speak with thick accents. Nothing could be further from the truth - they are elite organizations composed of well-educated and sophisticated individuals. An important first step toward countering the spy threat is NOT to underestimate their capabilities.

Another point to remember is that an operative of a foreign intelligence service need not be a foreigner, nor need the occasion of an encounter with him or her be in any way extraordinary. A routine acquaintance, for example, could turn out to be a diplomat from Eastern Europe or an American who has been recruited as an agent by a hostile intelligence service. He could be a "spotter," reporting to an intelligence service on persons who appear to be susceptible to recruitment, and arranging for intelligence officers to meet them.

Do not expect either the intelligence officer or agent to expose his role in any dramatic or sudden fashion. Usually there is a long period of cultivation during which conversations appear completely innocuous. At any point where an individual begins to inquire aggressively into aspects of your knowledge or activity, which are classified or otherwise sensitive, you should certainly stop to consider whether the inquiry is normal, innocent curiosity. It might be the beginning of an attempt to secure sensitive information for the benefit of another country.

It is important to recognize when an association evolves from one of strictly business to one of a more personal nature. In recruitment scenarios, a key first step taken by intelligence officers is the development of a personal rapport and social relationship with targeted individuals. This must be recognized. Casual meetings away from the office should not be solicited or accepted. One further defensive technique is to avoid one-on-one meetings. The more people involved in a meeting, the less opportunity there is for an intelligence officer to develop a personal rapport or to ask the employee questions he does not want to answer.

If an employee (especially if an individual has access to classified information) has dealings with representatives from the Soviet Union, Bloc countries, Cuba, or the People's Republic of China, there are a number of defensive steps that can be taken. The most important step is to have all such contacts reported to a Security Officer. This allows the Security Officer to monitor the contacts and to protect the employee's record.

The role of the Security Officer must be stressed. Each Government agency and private firm that deals in classified material has, or should have, a specified official responsible for security matters. This Security Officer should be recognized as an ally and not an adversary. If you become involved in a situation that arouses your suspicions, the Security Officer should be informed immediately. His job is to minimize damage that results from the loss of sensitive

information, protect employees from getting ensnarled in situations involving hostile intelligence services, and to extricate them when necessary. This assistance cannot be rendered if the employee remains silent. Of course, it is much better for an employee to reveal a suspected relationship voluntarily than have it come to light in the course of an investigation. In sum, if you become involved in a compromising situation, the sooner you consult your Security Officer, the better for all concerned: the employee, the employer, and the United States.

You may be in a place or situation where you cannot or, for some reason, do not want to contact your Security Officer. In the United States, the FBI is as close as your nearest telephone. Abroad, the nearest U. S. diplomatic establishment can arrange to put you in touch with the FBI or other appropriate U. S. Government security officials. Once again, it must be stressed that your best course of action in any of the situations described above is to relate the facts to a professional who will be able to analyze the situation and propose a course of action. Any attempts by untrained or uninformed persons to handle hostile approaches on their own could result not only in personal disaster, but may also interfere with the FBI's counterintelligence effort.

The threat posed by foreign intelligence services can easily be underestimated. History is replete with situations in which a nation's security was gravely damaged by the efforts of another nation's intelligence service. In our own history, the breaking of the Japanese secret code helped bring U. S. victory in the Pacific during World War II. On the other hand, the theft of some of our key atomic secrets greatly abetted the interests of the Soviet Union and threatened our national security. Intelligence activity is by no means trivial; the fate of nations can be affected.

The United States can be weakened by the theft of its vital scientific, technological, political, and military knowledge. Its enemies can be strengthened by the acquisition of that knowledge, whether classified or unclassified. It is the responsibility of all of us, who have been entrusted with sensitive data, to do our share in protecting the national security. If Americans do not conduct themselves in a responsible manner, or do not recognize that this country's national security is based upon the loyalty and efforts of its citizens, then the tightest document classification system, the most efficient security organizations, or the strongest armed forces may be completely ineffective in protecting its citizens.

"The only thing necessary
for the triumph of evil is
for good men to do nothing."

Edmund Burke

SAMPI APPEN X DD
RY/EXI INSP T ON GN

NOTICE

ALL PERSONNEL ENTERING
OR EXITING THIS FACILITY
ARE SUBJECT TO AN INSPECT ON
OF ALL HAND HELD TEMS

THIS INSPECTION IS IN
ACCORDANCE WITH THE
PROV SIONS OF PARAGRAPHS
5 300 5 301 AND 5-302
AR 380 5

APPENDIX EE

RECORD OF ISSUE OF DD FORM 2501

_____

(ACTIVITY)

CARD NUMBER	NAME	GRADE	DIVISION	DATE OF ISSUE*

* DD FORM 2501 VALID FOR ONE YEAR FROM THIS DATE

FSH FORM 252**(Restricted)
1 Aug 89 (DPTMSEC)